BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 25/2013
November 2013

Vorschlag der Bundesrechtsanwaltskammer

zum Vorschlag einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Daten-schutz-Grundverordnung)

Anlagen:
1. Änderungsanträge zu Art. 14 Datenschutz-Grundverordnung
2. Änderungsanträge zu Art. 15 Datenschutz-Grundverordnung
3. Änderungsanträge zu Art. 84 Datenschutz-Grundverordnung
4. Änderungsanträge zu Art. 80 Datenschutz-Grundverordnung

Mitglieder des Ausschusses Datenschutzrecht
RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Christel Hahne
RA Prof. Dr. Armin Herb
RA Dr. Hans Klees
RA Stephan Kopp
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Dr. Ralph Wagner, LL.M.
RAin Friederike Lummel, BRAK
RAin Valérie Gläß, BRAK

Verteiler:
Europäische Kommission
Bundesministerium der Justiz
Bundesministerium des Inneren
Landesjustizminister/Justizsenatoren der Länder
Bundesnotarkammer
Bundessteuerberaterkammer
Wirtschaftsprüferkammer
Deutscher Notarverein
Deutscher Anwaltverein
Redaktion der Neuen Juristischen Wochenschrift/NJW

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit etwa 161.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Die Bundesrechtsanwaltskammer begrüßt zunächst, dass der LIBE Ausschuss des Europäischen Parlaments die von ihr vorgeschlagenen Änderungen zu Art. 14, 15 und 84 der Datenschutz-Grundverordnung (**Anlagen 1 – 3**) für die anwaltlichen Berufsgeheimnisträger angenommen hat und in die Trilog-Verhandlungen einbringen wird. Sie sieht jedoch nach wie vor Änderungsbedarf im Hinblick auf die Ausgestaltung der Aufsichtsbehörden und fordert deshalb weiterhin die Einrichtung einer **sektoralen Datenschutzaufsicht für die Anwaltschaft**. Eine Ergänzung des bisherigen Art. 49 Datenschutz-Grundverordnung ist erforderlich, um einen lückenlosen Schutz der Verschwiegenheitspflicht der europäischen Rechtsanwältinnen und Rechtsanwälten zu gewährleisten.

I.

Die anwaltliche Verschwiegenheitspflicht wird sowohl auf mitgliedstaatlicher, als auch auf europäischer Ebene durch unterschiedliche Rechtssätze geschützt (vgl. BRAK-Stellungnahme 53/2012, 30/2012).

Das Recht auf effektive Verteidigung wurde auf europäischer Ebene durch den EuGH als allgemeiner Rechtsgrundsatz anerkannt (EuGH, Rs. C-7/98, Slg. 2000, I-1935, Rn. 38 - Dieter Krombach/André Bamberski). Dabei wurde ausdrücklich die Notwendigkeit der Vertraulichkeit des Schriftverkehrs zwischen dem Bevollmächtigten und seinem Mandanten betont (EuGH, Rs. 155/79, Slg 1982, 1575, Rn. 21 - AM&S Europe Ltd/Kommission). Durch die am 01.12.2009 in Kraft getretene europäische Grundrechte-Charta ist die anwaltliche Verschwiegenheit auf europäischer Ebene zudem als justizielles Grundrecht anerkannt worden. Gemäß Art. 47 Abs. 2 Satz 2 EU-Charta gilt: „Jede Person kann sich beraten, verteidigen und vertreten lassen." In Verbindung mit Art. 6 Abs. 1 EUV gehört das Recht auf anwaltliche Verschwiegenheit und Beratung zum geltenden europäischen Primärrecht. Es entfaltet damit für alle Rechtsakte des sekundären Gemeinschaftsrechts, wie z. B. die Datenschutz-Grundverordnung, unmittelbare Wirkung.

Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) umfasst der Begriff „faires Verfahren" des Art. 6 Abs. 1 EMRK verschiedene Elemente, zu denen u. a. die Rechte der Verteidigung, der Grundsatz der Waffengleichheit, das Recht auf Zugang zu den Gerichten sowie das Recht auf einen Rechtsanwalt sowohl in Zivil- als auch in Strafsachen gehören.

Das Gebot der Verschwiegenheit gehört zudem zu den tragenden Säulen des Anwaltsberufs in Europa. Nach 2.3 CCBE (Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers, 2.3 –„Confidentiality") zählt das Berufsgeheimnis zu den Grundpflichten und –rechten jedes europäischen Rechtsanwalts.

II.

Aufgrund der besonderen Bedeutung der anwaltlichen Verschwiegenheit für das Vertrauensverhältnis zwischen Rechtsanwalt und Mandant bedarf sie eines besonderen Schutzes vor staatlichen Eingriffen. Das Institut der Verschwiegenheitspflicht dient nicht den Interessen der Anwaltschaft, sondern schützt den Mandanten. Seine Aufweichung oder Durchbrechung führt dazu, dass Mandanten sich ihren anwaltlichen Vertretern nicht mehr uneingeschränkt anvertrauen können. Rechtsanwälte können dann die Interessen ihrer Mandanten weder gegenüber privaten Dritten noch gegenüber Behörden, Gerichten oder anderen staatlichen Organisationen sachgerecht vertreten. Damit wird durch die anwaltliche

Verschwiegenheitspflicht aber nicht nur das Individualinteresse des Mandanten, sondern auch das Interesse der Allgemeinheit an einer geordneten Rechtspflege geschützt. Beides kann jedoch nur aufrechterhalten werden, wenn sichergestellt ist, dass staatliche Eingriffe in den Vertrauensbereich Anwalt - Mandant ausgeschlossen sind. Dieser Aufgabe kann sich kein Staat, der sich einer freiheitlich-demokratischen Rechtsordnung verpflichtet sieht, entziehen.

III.

Die in der Datenschutz-Grundverordnung vorgesehene Regelung zu Art. 49 genügt nicht den vorstehenden Anforderungen. Die Bundesrechtsanwaltskammer bekräftigt deshalb ihre bislang schon bekundete Auffassung zu ihrer Ergänzung. Art. 49 legt den Mitgliedsstaaten in der aktuellen Fassung die Verpflichtung auf, innerhalb ihrer nationalen Verwaltungen territoriale Datenschutzkontrollstellen einzurichten. Eine sektorale Kontrollstelle für Berufsgeheimnisträger ist nicht vorgesehen.

Die Bundesrechtsanwaltskammer schlägt vor, Art. 49 in einem Abs. 2 wie folgt zu ergänzen:

> ***„Soweit für die Berufsaufsicht von Berufsgeheimnisträgern zum Zeitpunkt des In-Kraft-Tretens dieser Verordnung zuständige Stellen bestehen, können diese die Aufsichtsbehörden errichten.“***

Die Einführung einer sektoralen Datenschutzkontrollstelle für Berufsgeheimnisträger, insbesondere für die Anwaltschaft wird den besonderen europarechtlichen Anforderungen, die für Rechtsanwälte (vgl. z. B. Art. 47 Satz 3 EU-Grundrechte-Charta) zu beachten sind, gerecht und steht im Einklang mit den anderen Vorschriften der Datenschutz-Grundverordnung.

1. Vereinbarkeit mit den europarechtlichen Anforderungen für Berufsgeheimnisträger

Zunächst wird sichergestellt, dass durch die Einrichtung einer sektoralen Datenaufsichtsbehörde keine staatlichen Eingriffe in das sensible Anwalt-Mandant-Verhältnis stattfinden. Die Aufsichtsbehörden für die Berufsgeheimnisträger können nämlich als unabhängige Stellen bei den Selbstverwaltungskörperschaften der Vertrauensberufe eingerichtet werden. In Deutschland könnte also ein Datenschutzbeauftragter für die Anwaltschaft bei der Bundesrechtsanwaltskammer angesiedelt werden. Bekannt sein dürfte, dass die Bundesrechtsanwaltskammer bereits als sektorale Aufsichtsbehörde im Rahmen des Geldwäschegesetzes (§ 16 Abs. 2 Nr. 4 GwG) fungiert.

Eine sektorale Datenschutzaufsicht hat darüber hinaus den Vorteil, dass zur Durchsetzung datenschutzrechtlicher Vorschriften zusätzlich zu den in der Verordnung vorgesehenen Regelungen die bestehenden berufsrechtlichen Sanktionsmittel herangezogen werden können. Sie gehen weit über die zurzeit angedachten Befugnisse der Aufsichtsbehörden hinaus.

Für die Mandanten bleiben ihre dem Berufsgeheimnisträger anvertrauten Daten im sektoralen Bereich ihrer Vertrauensperson und fallen nicht in die Beurteilung einer staatlichen Behörde, womit zusätzlich eine fachspezifische Interpretation und Bewertung der Datenverarbeitung gewährleistet wird. Berufsgeheimnisse und Verschwiegenheitspflichten bleiben erhalten, weil nur Berufsgeheimnisträger selbst tätig sind.

Eine sektorale Datenaufsicht ist zudem aus Gründen des Verbraucherschutzes zu begrüßen: Bei der Einrichtung eines zentralen Datenschutzbeauftragten der Anwaltschaft erhält der Rechtssuchende einen zentralen Ansprechpartner für seine Belange.

2. Vereinbarkeit mit den Anforderungen aus der Datenschutz-Grundverordnung

Art. 49 der Datenschutz-Grundverordnung sieht schon jetzt vor, dass mehrere Aufsichtsbehörden innerhalb eines Mitgliedsstaates mit der Überwachung des Datenschutzes betraut werden können.

Der in Art. 84 verankerte Subsidiaritätsgedanke spricht in Umsetzung dieser Vorgabe für die Einführung einer sektoralen Datenschutzkontrolle für Berufsgeheimnisträger. Die Bestimmung selbst befugt die Mitgliedsstaaten, abweichende Regelungen für die Kontrollbefugnisse des Datenschutzbeauftragten im Hinblick auf die besondere Stellung der Berufsgeheimnisträger zu erlassen. Hierdurch wird deutlich, dass die Europäische Kommission die Problematik der Kollision zwischen der Verschwiegenheitspflicht bei Berufsgeheimnisträgern und dem Datenschutzrecht gesehen hat. Die Regelung trägt diesem Konflikt aber nicht hinreichend Rechnung. Denn um den absoluten Schutz des europäischen Anwaltsprivilegs sicherzustellen, bedarf es einer vom Staat und von der Anwaltschaft unabhängigen Stelle, die ihre Befugnisse frei von sonstigen Weisungen wahrnimmt. Die Zuteilung besonderer Rechte (gem. Art. 84) an einen staatlichen Datenschutzbeauftragten kann den erforderlichen Schutz nicht sicherstellen, da bereits dort zeitlich und räumlich der Zugriff anderer Personen auf die zu schützenden Unterlagen möglich wäre.

Ein Datenschutzbeauftragter der Anwaltschaft kann – den Vorgaben der Datenschutz-Grundverordnung folgend – in überzeugender Weise auch personell unabhängig tätig werden: Seine Bestellung könnte sich an der des Bundesdatenschutzbeauftragten gem. § 22 BDSG orientieren. Die BRAK könnte dem Bundestag einen oder bis zu drei geeignete Kandidaten vorschlagen, die die fachlichen und persönlichen Kriterien erfüllen, die an die Person des Datenschutzbeauftragten der Anwaltschaft zu stellen sind. Das Parlament könnte sodann über die Bestellung entscheiden.

Um seine persönliche Unabhängigkeit zu sichern, könnte entsprechend der Amtszeit eines Bundesverfassungsrichters die des Datenschutzbeauftragten der Anwaltschaft zwölf Jahre ohne Möglichkeit der Wiederwahl betragen. Die Wählbarkeit könnte an die Wahl zum Bundesverfassungsrichter anknüpfend ein Mindestalter von 40 Jahren und eine Tätigkeit als Rechtsanwalt von mindestens fünf Jahren voraussetzen, um so die anwaltsspezifische Expertise zu gewährleisten. Der Datenschutzbeauftragte der Anwaltschaft dürfte während der Ausübung seiner Funktion nicht anwaltlich tätig sein. Insoweit sollte eine strenge Inkompatibilitätsregelung gelten. Es sollte zudem entsprechend § 4 BVerfGG eine Altersgrenze von 68 Jahren geben.

Es könnte zudem sichergestellt werden, dass nur in Ausnahmefällen das Amt vorzeitig aufgegeben werden kann. Entsprechend den für Bundesverfassungsrichter geltenden Regelungen sollte der Datenschutzbeauftragte der Anwaltschaft nur in konkret geregelten Fällen und in einem gesetzlich bestimmten Verfahren aus dem Amt entfernt werden können. Analog § 105 BVerfGG sollte im Falle dauerhafter Dienstunfähigkeit der BRAK-Präsident ermächtigt werden, ihn in den Ruhestand zu versetzen. Außerdem könnte eine rechtskräftige Verurteilung wegen einer strafbaren Handlung oder eine grobe Pflichtverletzung eine Entlassung rechtfertigen.

Durch diese Ausgestaltung könnte eine im Sinne der Verordnung und der europäischen Rechtsprechung unabhängige, fachkundige und bundeseinheitlich eingerichtete Stelle und gleichzeitig eine die speziellen Anforderungen des Berufsgeheimnisses wahrende Datenschutzkontrolle gewährleistet werden. Das Konzept ist dem vorliegenden Vorschlag im Übrigen nicht fremd. Es wird bereits für andere grundrechtsrelevante Lebensbereiche, z. B. für die Kirchen und für die Medien (vgl. Art. 80 der Datenschutz-Grundverordnung in der vom LIBE-Ausschuss ergänzten Fassung, **Anlage 4**), vorgesehen. Es für die Rechtspflege und damit für die grundrechtlich geschützte Vertrauensbeziehung zwischen Rechtsanwalt und Mandant zu übernehmen, ist zwingend geboten.

* * *

Anlage 1
Änderungsanträge zu Art. 14 Datenschutz-Grundverordnung

COMP Article 14
17.10.2013

Article 14
Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information, ***after the particulars pursuant to Article 13a have been provided***:

(a) the identity and the contact details of the controller and, if any, of the controller's representative, of the data protection officer;

(b) the purposes of the processing for which the personal data are intended, ***as well as information regarding the security of the processing of personal data***, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and ~~***the legitimate interests pursued by the controller***~~, ***where applicable, information on how they implement and meet the requirements of point f of Article 6(1)***;

(c) the period for which the personal data will be stored, ***or if this is not possible, the criteria used to determine this period***;

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject to object to the processing of such personal data, ***or to obtain data***;

(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(f) the recipients or categories of recipients of the personal data;

(g) where applicable, that the controller intends to transfer ***the data*** to a third country or international organisation and on ~~***the level of protection afforded by that third country or international organisation by reference to***~~ ***the existence or absence of*** an adequacy decision by the Commission, ***or in case of transfers referred to in Article 42, Article 43, or point (h) of Article 44(1), reference to the appropriate safeguards and the means to obtain a copy of them***;

(ga) where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;

(gb) meaningful information about the logic involved in any automated processing;

(h) any further information ***which is*** necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected ***or processed, in particular the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk;***

(ha) where applicable, information whether personal data was provided to public authorities during the last consecutive 12-month period.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is ~~*obligatory*~~ ***mandatory*** or ~~*voluntary*~~ ***optional***, as well as the possible consequences of failure to provide such data.

2a. In deciding on further information which is necessary to make the processing fair under 1(h), controllers shall have regard to any relevant guidance under Article 38.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the ***specific*** personal data originate. ***If personal data originates from publicly available sources, a general indication may be given.***

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) at the time when the personal data are obtained from the data subject ***or without undue delay where the above is not feasible***; or

(aa) on request by a body, organization or association referred to in Article 73;

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a ~~*disclosure*~~ ***transfer*** to another recipient is envisaged, and at the latest ~~*when the data are first disclosed*~~ ***at the time of the first transfer, or, if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject; or***

(bb) only on request where the data are processed by a small or micro enterprise which processes personal data only as an ancillary activity.

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

(b) the data ***are processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83,*** are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort ***and the controller has published the information for anyone to retrieve***; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law ***to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests, considering the risks represented by the processing and the nature of the personal data***; or

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others ***natural persons***, as defined in Union law or Member State law in accordance with Article 21.

(da) the data are processed in the exercise of his profession by, or are entrusted or become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation of secrecy, unless the data is collected directly from the data subject.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's ***rights or*** legitimate interests.

~~***7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.***~~

~~***8. The Commission shall lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary*** *as well as the needs of the relevant stakeholders.* ***Those implementing acts shall be adopted, after requesting an opinion of the European Protection Board, in accordance with the examination procedure referred to in Article 87(2).***~~

Recitals

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be ***likely*** stored ***for each purpose, if the data are to be transferred to third parties or third countries,*** on the existence ***of measures to object and*** of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data. ***This information should be provided, which can also mean made readily available, to the data subject after the provision of simplified information in the form of standardised icons.***

(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.

(50) However, it is not necessary to impose this obligation where the data subject already ~~***disposes of***~~ ***knows*** this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves

impossible or would involve disproportionate efforts. ~~*The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.*~~

Anlage 2
Änderungsanträge zu Art. 15 Datenschutz-Grundverordnung

COMP Article 15 and 18
16.10.2013

Article 15
Right to access and to obtain data for the data subject

1. ***Subject to Article 12(4),*** the data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed, ***and in clear and plain language,*** the following information:

(a) the purposes of the processing ***for each category of personal data;***

(b) the categories of personal data concerned;

(c) the recipients ~~***or categories of recipients***~~ to whom the personal data are to be or have been disclosed, ~~***in particular***~~ ***including*** to recipients in third countries;

(d) the period for which the personal data will be stored***, or if this is not possible, the criteria used to determine this period***;

(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

~~***(g) communication of the personal data undergoing processing and of any available information as to their source;***~~

(h) the significance and envisaged consequences of such processing~~***, at least in the case of measures referred to in Article 20***~~.

(ha) meaningful information about the logic involved in any automated processing;

(hb) without prejudice to Article 21, in the event of disclosure of personal data to a public authority as a result of a public authority request, confirmation of the fact that such a request has been made.

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in ***an*** electronic ***and structured*** format, unless otherwise requested by the data subject. ***Without prejudice to Article 10, the***

controller shall take all reasonable steps to verify that the person requesting access to the data is the data subject.

2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.

2b. This Article shall be without prejudice to the obligation to delete data when no longer necessary under Article 5(1)(e).

2c. There shall be no right of access in accordance with paragraphs 1 and 2 when data within the meaning of Article 14(5)(da) are concerned, except if the data subject is empowered to lift the secrecy in question and acts accordingly.

~~*3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.*~~

~~*4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

~~*Article 18*~~
~~*Right to data portability*~~

~~*1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.*~~

~~*2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.*~~

~~*3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Recitals

(51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what ***estimated*** period, which recipients receive the data, what is the ***general*** logic of the data that are undergoing the processing and what might be~~*, at least when based on profiling,*~~ the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property, ***such as in relation to*** ~~*and in particular*~~ the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

~~*(55)*~~*(51a)* To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. ***Data controllers should be encouraged to develop interoperable formats that enable data portability.*** This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract. ***Providers of information society services should not make the transfer of those data mandatory for the provision of their services.***

Anlage 3
Änderungsanträge zu Art. 84 Datenschutz-Grundverordnung

COMP Article 84
7.10.2013

Article 84
Obligations of secrecy

1. ***In accordance with the rules set out in*** this Regulation, Member States ~~***may adopt***~~ ***shall ensure*** specific rules ***are in place setting set*** out the ~~***investigative***~~ powers by the supervisory authorities laid down in Article 53~~***(2)***~~ in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Recitals

(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.

Anlage 4
Änderungsanträge zu Art. 80 Datenschutz-Grundverordnung

COMP AM Article 80
15.10.2013

Article 80
Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI, ~~***and***~~ on co-operation and consistency in Chapter VII ***and specific data processing situations in Chapter IX whenever this is necessary*** ~~***for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression***~~ in order to reconcile the right to the protection of personal data with the rules governing freedom of expression ***in accordance with the Charter of Fundamental Rights of the European Union***.

2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

Recitals

(121) ***Whenever necessary, exemptions or derogations*** ~~***The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption***~~ from the requirements of certain provisions of this Regulation for the processing of personal data ***should be provided for*** in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. ~~***This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries.***~~ Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities***,*** ~~***and***~~ on co-operation and consistency***, and on specific data processing situations***. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom~~***, such as journalism,***~~ broadly ~~***Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of***~~ ***to cover all these*** activities ***which aim at is*** the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them, ***also taking into account technological development***. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.